

1 JOHN A. YANCHUNIS (*pro hac vice*)
2 jyanchunis@forthepeople.com
3 JONATHAN B. COHEN (*pro hac vice*)
4 jcohen@forthepeople.com
5 RYAN J. McGEE (*pro hac vice*)
6 rmcgee@forthepeople.com
7 **MORGAN & MORGAN**
8 **COMPLEX LITIGATION GROUP**
9 201 N. Franklin Street, 7th Floor
10 Tampa, Florida 33602
11 Telephone: (813) 223-5505
12 Facsimile: (813) 223-5402

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

*Counsel for Plaintiffs Matt Matic and
Zak Harris*

IVY T. NGO, SBN 249860
ngoi@fdazar.com
FRANKLIN D. AZAR & ASSOCIATES, P.C.
14426 East Evans Avenue
Aurora, Colorado 80014
Telephone: (303) 757-3300
Facsimile: (720) 213-5131

*Counsel for Plaintiffs Charles Olson and
Eileen M. Pinkowski*

Clayeo C. Arnold, SBN 65070
carnold@justice4you.com
Joshua H. Watson, SBN 238058
jwatson@justice4you.com
CLAYEO C. ARNOLD
A PROFESSIONAL LAW
CORPORATION
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE GOOGLE PLUS PROFILE
LITIGATION

Case No. 5:18-cv-06416-EJD (VKD)

**AMENDED CONSOLIDATED CLASS
ACTION COMPLAINT**

Judge: Hon. Edward J. Davila
Date Filed: October 8, 2018
Lead Counsel Hearing: March 14, 2019
Trial Date: None set

TABLE OF CONTENTS

2	SUMMARY OF THE CASE.....	1
3	JURISDICTION AND VENUE	2
4	PARTIES	3
5	A. Plaintiffs.....	3
6	FACTUAL BACKGROUND	4
7	A. Defendant Made Specific Representations to Users Regarding	
8	Defendant’s Protection of Users’ Personal Information	4
9	B. Google’s Inadequate Data Security Allowed for the First Data Leak	
10	Which Was Intentionally Concealed from the Public for Over Seven	
11	Months	6
12	C. Defendant’s Business Decision to Not Immediately Disclose the First	
13	Data Leak Put Their Interests Above That of Google+ Users and	
14	Exacerbated the Harm Caused.....	9
15	D. Defendant Failed to Properly Secure Google+ After the First Data	
16	Leak, Resulting in the Exposure of Even More Users’ Personal	
17	Information in the Second Data Leak	12
18	E. Users’ Personal Information Is an Increasingly Valuable Commodity	13
19	F. Google Has A Long History of Improper Data Practices	17
20	PLAINTIFFS’ FACTUAL ALLEGATIONS	18
21	CLASS ACTION ALLEGATIONS	23
22	First Claim for Relief.....	27
23	Violation of California’s Unfair Competition Law (“UCL”) – Unlawful Business	27
24	Practice (Cal. Bus. & Prof. Code § 17200, <i>et seq.</i>).....	27
25	Second Claim for Relief.....	29
26	Violation of California’s UCL – Unfair Business Practice	29
27	(Cal. Bus. & Prof. Code § 17200, <i>et seq.</i>)	29
28	Third Claim for Relief	32
29	Violation of California’s UCL – Fraudulent/Deceptive Business Practice	32
30	(Cal. Bus. & Prof. Code § 17200, <i>et seq.</i>)	32
31	Fourth Claim for Relief.....	33

1	Negligence	33
2	Fifth Claim for Relief.....	35
3	Invasion of Privacy	35
4	Sixth Claim for Relief.....	36
5	Breach of Confidence	36
6	Seventh Claim for Relief	38
7	Deceit by Concealment or Omission	38
8	(Cal. Civil Code §§ 1709, 1710).....	38
9	Eighth Claim for Relief.....	40
10	Breach of Contract	40
11	Ninth Claim for Relief	41
12	Breach of Implied Covenant of Good Faith and Fair Dealing.....	41
13	(In the Alternative).....	41
14	PRAAYER FOR RELIEF	42
15	JURY TRIAL DEMANDED.....	43
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

For their Amended Consolidated Class Action Complaint, Plaintiffs Matt Matic, Zak Harris, Charles Olson, and Eileen M. Pinkowski (collectively “Plaintiffs”) on behalf of themselves and all others similarly situated, allege the following against Defendant Google LLC (“Defendant” or “Google”), based on personal knowledge as to Plaintiffs and Plaintiffs’ own acts and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through Plaintiffs’ undersigned counsel:

SUMMARY OF THE CASE

1. This case involves two related data leaks affecting millions of people who have used Defendant’s Google+ social network. The first data leak, which Defendant knew about for months before announcing it on October 8, 2018, involves the improper exposure of the personal information of at least 500,000 Google+ users (“Google+ Users” or “Users”) due to a software glitch that gave third-party application developers access to private Google+ profile data between 2015 and March 2018 (the “First Data Leak”). The second data leak, as Defendant disclosed just over two months later on December 10, 2018, similarly involves the improper exposure of the personal information of Users to third-party application developers, except this time, ***at least 52.5 million Users*** were affected (the “Second Data Leak”). These data leaks are collectively referred to herein as the “Google+ Data Leaks.”

2. Launched in June 2011, Google+ (or Google Plus) is a social network owned and operated by Google for consumers with Google accounts. Google+ facilitates the sharing of information, photographs, weblinks, conversations, and other shared content similar in many respects to the Facebook news feed or Twitter stream. Google+ replaced Google's previous social network effort, Google Buzz, after the platform faced lawsuits and an action by the Federal Trade Commission ("FTC") concerning users' numerous privacy concerns with the platform, including alleged misrepresentations regarding Google's privacy assurances to users.

3. As part of the sign-up process and as a consequence of interacting with the network, Google+ Users create, maintain, and update profiles containing significant amounts of Personal Information, including their names, birthdates, hometowns, addresses, locations,

1 interests, relationships, email addresses, photos, and videos, amongst other information
2 (“Personal Information”).

3 4. Google maintains a privacy policy that makes specific representations to its users
4 regarding its affirmative duty to protect users' Personal Information, specifically providing that
5 users are in control of who has access to their Personal Information ("Privacy Policy").

6 5. When a User adds a contact to his or her Google+ account, the User assigns that
7 person to one or more “circles” in order to categorize or organize the contact. Google+ Users
8 determine privacy settings for content they share on Google+, allowing content to be shared
9 with the public or with only those people in their designated circles.

10 6. While Users' Personal Information was supposed to be protected and shared only
11 with their expressed permissions and limitations, Defendant allowed third-party application
12 developers to improperly collect the Personal Information of at least 500,000 Google+ Users in
13 the First Data Leak.

14 7. Instead of choosing to be transparent about the First Data Leak, Defendant
15 explicitly chose to conceal it from the public until after the public outcry following Facebook's
16 widely publicized Cambridge Analytica scandal had diminished – hoping to avoid both public
17 and Congressional scrutiny.

18 8. Then, just over two months after Defendant's announcement of the First Data
19 Leak, Defendant announced the Second Data Leak, whereby the Personal Information of Users
20 was, *again*, improperly exposed to third-party applications developers. But this time, *at least*
21 **52.5 million Users** were impacted.

22 9. This Amended Consolidated Class Action Complaint is filed on behalf of all
23 persons in the United States, described more fully *infra*, whose Personal Information was
24 compromised in the Google+ Data Leaks.

JURISDICTION AND VENUE

26 10. This Court has jurisdiction over this action pursuant to the Class Action Fairness
27 Act (“CAFA”), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds
28 \$5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least

1 one class member is a citizen of a state different from Defendant. The Court also has
 2 supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1337.

3 11. Venue is proper under 28 U.S.C. § 1331(c) because Defendant is a corporation
 4 that does business in and is subject to personal jurisdiction in this District. Venue is also proper
 5 because a substantial part of the events or omissions giving rise to the claims in this action
 6 occurred in or emanated from this District, including the decisions made by Defendant's
 7 governance and management personnel that led to the Google+ Data Leaks and the decision not
 8 to disclose the First Data Leak earlier.

9 12. Further, the venue provision in Google's Terms of Service governing users in the
 10 United States provides an additional reason that venue is proper in this District. That provision
 11 provides for venue in the Northern District of California for all claims arising out of Plaintiffs'
 12 relationship with Google.

13 13. The Terms of Service also provide that all claims that might arise between Users
 14 and Defendant would be governed by the laws of California, without regard to conflict-of-law
 15 provisions. Accordingly, the choice-of-law provision establishes that California law applies to
 16 Plaintiffs' and the other Class Members' claims.

17 **PARTIES**

18 **A. Plaintiffs**

19 14. Plaintiff Matt Matic is a resident and citizen of California. Mr. Matic opened a
 20 Google+ account in 2014 and has used his account throughout the relevant time period.

21 15. Plaintiff Zak Harris is a resident and citizen of Florida. Mr. Harris opened a
 22 Google+ account in 2011 and has used his account throughout the relevant time period.

23 16. Plaintiff Charles Olson is a resident and citizen of Colorado. Mr. Olson opened a
 24 Google+ account in 2014 and has used his account throughout the relevant time period.

25 17. Plaintiff Eileen M. Pinkowski is a resident and citizen of Colorado. Ms.
 26 Pinkowski opened a Google+ account in 2011 and has used her account throughout the relevant
 27 time period.

B. Defendant

18. Defendant Google LLC (“Google”) is a Delaware corporation with its principal headquarters in Mountain View, California.

19. At all relevant times, Defendant was and is engaged in business in San Mateo County and throughout the United States of America.

FACTUAL BACKGROUND

A. Defendant Made Specific Representations to Users Regarding Defendant's Protection of Users' Personal Information

20. Google's Terms of Service make it clear that Google collects information from its users.¹ However, at all relevant times, Google has maintained a Privacy Policy that makes specific representations to Users regarding its protection and exposure of their Personal Information.²

21. The Google Privacy Policy specifically advises Users that: “When you use our services, you’re ***trusting us*** with your information.³ We understand this is a ***big responsibility*** and work hard to protect your information and put ***you*** in control.” Further, Google represents that “We’ll share Personal Information outside Google ***when we have your consent.***⁴

22. Other specific representations to Users in the Google Privacy Policy include:

1. “You have choices regarding the information we collect and how it’s used.”⁵
2. “We’ll ask for your consent before using your information for a purpose that isn’t covered in this Privacy Policy.”⁶
3. “We’ll ask for your *explicit* consent to share any sensitive personal information.”⁷

23. And importantly for the Google+ Data Leaks, Google represents to its users they can “[c]ontrol whom you share information with through your account on Google+.”⁸

¹ Google, *Terms of Service* (October 25, 2017), <https://policies.google.com/terms?hl=en&gl=ZZ> (last visited December 11, 2018).

² Google, *Privacy Policy* (May 25, 2018), <https://policies.google.com/privacy> (last visited December 11, 2018).

³ *Id* (emphasis added).

⁴ *Id* (emphasis added).

5 *Id*

10.

⁷ *Id.* (emphasis added)

1 24. Despite these representations, Google's lax approach to data security resulted in
 2 the Google+ Data Leaks affecting at least 53 million Google+ users over a period of at least 3
 3 years.⁹

4 25. Likewise, Google has specifically disclosed that it owes a duty to Users to timely
 5 inform them of breaches involving private personal data, like the Personal Information exposed
 6 in the Google+ Data Leaks. On December 11, 2018, Google CEO Sundar Pichai was called to
 7 testify before the House Judiciary Committee on the various privacy and antitrust issues
 8 plaguing Google, including the Google+ Data Leaks.¹⁰ During an exchange with Congressman
 9 Jerrold Nadler (D-NY), in a direct reference to the Google+ Data Leaks, Mr. Pichai admitted
 10 that Google understood that it needed to notify impacted Users within **72 hours** of ascertaining
 11 who the Users are:

12 **Jerrold Nadler (D-NY):** According to media reports Google found evidence that
 13 – well, let me go to the other one first. Google found a bug in its Google Plus
 14 social media platform that could have potentially exposed the private data of up
 15 to half a million users without the consent to third-party developers. Google
 16 however did not disclose this bug until months later after it was revealed by a
 17 report in the Wall Street Journal. Yesterday, as I mentioned before, they found –
 18 you announced another bug. *What legal obligations is the company under to
 19 disclose data exposures that do not involve sensitive financial information, but
 20 still involve private personal data, like users' name, age, email address or
 21 phone number. . . .*

22 **Sundar Pichai (CEO – Google):** Today, right now, if you've found a bug – you
 23 know, and you've ascertained – once you've done the investigation and you've
 24 ascertained the users who are eligible for notification, my understanding is **you
 25 have 72 hours**, and we both notify users as well as regulators in that
 26 timeframe.¹¹

27

⁸ *Id.*

28 ⁹ The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*
 29 (October 8, 2018), available at <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194> (last visited December 11, 2018); The Wall Street Journal, *Google to Accelerate Closure of Google+ Social Network After Finding New Software Bug* (December 10, 2018), available at <https://www.wsj.com/articles/google-to-accelerate-closure-of-google-social-network-1544465975> (last visited December 11, 2018).

29 ¹⁰ C-SPAN, *Google Data Collection* (December 11, 2018) available at <https://www.c-span.org/video/?455607-1/google-ceo-sundar-pichai-testifies-data-privacy-bias-concerns> (last visited December 18, 2018).

30 ¹¹ *Id.* at 41:00.

1 26. Despite Mr. Pichai's representations of Defendant's duty of timely disclosure,
 2 Defendant hid the First Data Leak from Users, the general public, and regulators for over 7
 3 **months.**

4 **B. Google's Inadequate Data Security Allowed for the First Data Leak Which
 5 Was Intentionally Concealed from the Public for Over Seven Months**

6 27. On October 8, 2018, Defendant announced that it would be permanently shutting
 7 down the consumer functionality of Google+.¹² Within this announcement, Defendant disclosed
 8 that a "software glitch" had allowed outside application (i.e. "app") vendors access to private
 9 Google+ User profile data between 2015 and March 2018.¹³

10 28. Google+ Users may allow third party applications to access their private profile
 11 data. But a "glitch" or "bug" in the Application Program Interfaces ("API") allowed third-party
 12 applications to access the personal profile data of other Google+ Users within the authorizing
 13 User's circles without User consent. Google represented that this vulnerability could have
 14 potentially affected at least half a million Google users from 2015 and May 2018.¹⁴

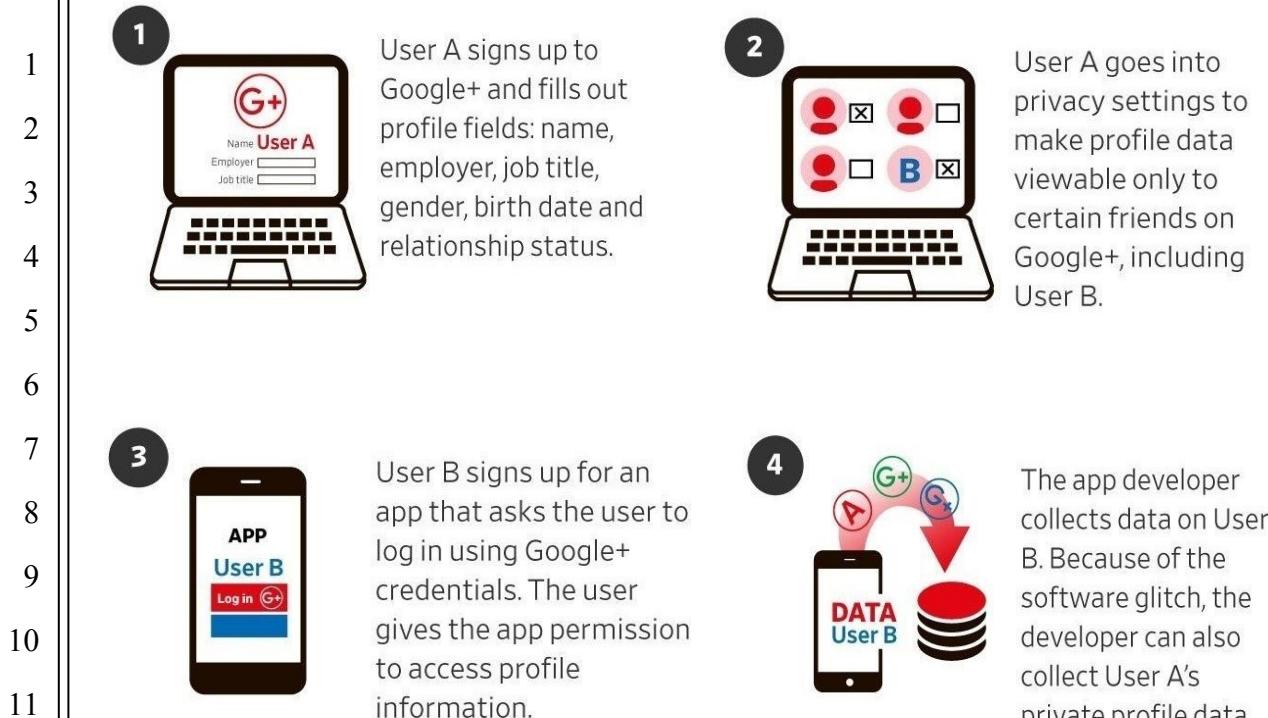
15 29. In sum, the First Data Leak made it possible for third parties to access private
 16 Personal Information about Users who never had an opportunity to consent to such access. The
 17 access allowed through this "glitch" is shown in the following illustration:

18
 19
 20
 21
 22
 23
 24

¹² Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+*, (October 8, 2018), available at <https://www.blog.google/technology/safety-security/project-strobe/> (last visited December 11, 2018); *see also* The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra* fn. 10.

¹³ Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+*, *supra* fn. 11.

¹⁴ The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra* fn. 10.



13 30. Defendant has advised that at least 438 third-party applications may have used
 14 the API related to the First Data Leak and thereby had been allowed unauthorized access to
 15 certain Google+ users' Personal Information for nearly 3 years.¹⁵

16 31. When the First Data Leak was disclosed, it immediately drew comparisons to
 17 Facebook's leak of user information to Cambridge Analytica and other third-party application
 18 developers.¹⁶ Given that Google+ was launched to challenge Facebook, the data security
 19 incidents suffered by Facebook users should have made Defendant more sensitive to the
 20 necessary protection of Google+ Users' data.

21 32. Instead, after discovering this vulnerability in the Google+ platform, Defendant
 22 kept silent for at least seven months, making a calculated decision to not inform Users that their
 23 Personal Information was compromised and allowing the unauthorized compromise of Users'

25 ¹⁵ Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer*
 26 *Google+*, *supra* fn. 11.

27 ¹⁶ The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra*
 28 fn. 10. See also The Washington Post, *Facebook: 'Malicious actors' used its tools to discover identities and collect*
data on a massive global scale (April 4, 2018), available at https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.61ae2fe14b0b (last visited December 11, 2018).

1 Personal information and their exposure to risk of identity theft or worse to continue during that
 2 time.

3 33. Although Defendant claimed in the blog post announcing the First Data Leak
 4 that they “found no evidence that any developer was aware of this bug, or abusing the API” or
 5 “that any Profile data was misused,” Defendant also represented that it only kept logs for two
 6 weeks.¹⁷ Thus, based on Defendant’s own admission that it can only account for whether the
 7 Google+ vulnerability had been exploited in the two weeks preceding its discovery, it has
 8 insufficient records to confirm whether and what data breaches had occurred during the three-
 9 year exposure period. As such, the full extent of the damage caused by Defendant’s failure to
 10 provide adequate controls and protection for Users’ Personal Information may never be known.
 11 Accordingly, the number of impacted Users, as well as the third-party applications that may
 12 have been able to exploit the Google+ vulnerability to access Users’ Personal Information, was
 13 likely significantly more than what Google disclosed – 500,000 Users and 438 third-party
 14 applications.

15 34. Plaintiffs’ gravest concerns proved true when Defendant announced the Second
 16 Data Leak just over two months later, which concerned similar-if-not-identical API, exposing
 17 the Personal Information of approximately 52.5 million Google+ Users – bringing the total
 18 potential exposure to 53 million Google+ Users.¹⁸

19 35. Although Defendant has represented that the Second Data Leak only existed
 20 from November 7, 2018 through November 13, 2018, Defendant has provided few details and
 21 still intend to operate the clearly bug-ridden and unsecure Google+ platform until April 2019.¹⁹

22 36. This case involves the absolute and intentional disregard with which Defendant
 23 has chosen to treat the Personal Information of Users who have utilized their Google+ social
 24

25 ¹⁷ Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer*
 26 *Google+*, *supra* fn. 11.

27 ¹⁸ The Wall Street Journal, *Google to Accelerate Closure of Google+ Social Network After Finding New*
 28 *Software Bug*, *supra* fn. 10.

29 ¹⁹ *Id.* See also Google, *Expediting changes to Google+* (December 10, 2018), available at
 28 https://www.blog.google/technology/safety-security/expediting-changes-google-plus/ (last visited December 11,
 29 2018).

1 media platform. While this Personal Information was supposed to be protected and shared only
 2 with expressed permissions, Defendant – without authorization – exposed that information to
 3 third parties through lax and non-existent data safety and security policies and protocols.

4 **C. Defendant’s Business Decision to Not Immediately Disclose the First Data
 5 Leak Put Their Interests Above That of Google+ Users and Exacerbated the
 6 Harm Caused**

7 37. Equally troubling to the widespread and unknown impact of the First Data Leak
 8 is Defendant’s intentional effort, approved by its upper management, to conceal the leak from
 9 the public and its victims.

10 38. When Defendant announced the First Data Leak, it shocked the public by
 11 revealing that it had discovered and “fixed” the security vulnerability in March 2018 – an
 12 astonishing seven months before the announcement.²⁰

13 39. According to the Wall Street Journal, a Google internal memorandum prepared
 14 by its legal and policy staff and shared with its senior executives revealed that Google had
 15 hidden the security vulnerability for six months to avoid public scrutiny about its privacy
 16 practices.²¹ According to that internal memorandum, Defendant’s decision not to disclose the
 17 Google+ vulnerability was motivated by the fear that doing so would draw “immediate
 18 regulatory interest,” bring Google “into the spotlight alongside or even instead of Facebook
 19 despite having stayed under the radar throughout the Cambridge Analytica scandal,” and
 20 “almost [guarantee that] Sundar [Pichai, Chief Executive Officer of Google,] will testify before
 Congress.”²²

21 40. Google’s failure to adequately disclose the Google+ vulnerability for months on
 22 end has made the regulatory and congressional interest in the data breach even greater than if
 23 Google had simply disclosed it when it was discovered. The First Data Leak has directly led to
 24 recent Congressional calls for investigation, including questions regarding Google’s compliance

25
 26 ²⁰ Google, *Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer*
Google+, *supra* fn. 11.

27 ²¹ The Wall Street Journal, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, *supra*
 28 fn. 10.

²² *Id.*

1 with the aforementioned FTC consent decree's requirements with respect to privacy settings and
 2 the protection of private information.²³

3 41. An October 11, 2018 letter to Mr. Pichai from Commerce Committee Chairman
 4 John Thune (R-S.D.) detailed Google's culture of concealment and opacity, noting that:

5 At the same time that Facebook was learning the important lesson that tech firms
 6 must be forthright with the public about privacy issues, Google apparently
 7 elected to withhold information about a relevant vulnerability for fear of public
 8 scrutiny. We are especially disappointed given that Google's chief privacy
 9 officer testified before the Senate Commerce Committee on the issue of privacy
 10 on September 26, 2018—just two weeks ago—and did not take the opportunity
 11 to provide information regarding this very relevant issue to the Committee.²⁴

12 42. In addition, an October 11, 2018 letter to Mr. Pichai from Senate Judiciary
 13 Committee Chairman Chuck Grassley not only detailed the obvious similarities between the
 14 First Data Leak and Facebook's widely publicized Cambridge Analytica scandal, but also
 15 reprimanded Google for its refusal to participate in past hearings on data breaches when it had
 16 concealed knowledge of the First Data Leak:

17 In March of this year, data privacy and social media was in the spotlight thanks
 18 to events surrounding Facebook and Cambridge Analytica. I convened a hearing
 19 with the CEO of Facebook on April 10, 2018, and according to his testimony, a
 20 feature in Facebook's application programming interface, or API, allowed third
 21 party developers to pull information not just from users of an application, but
 22 also that user's friends, even if the friend had made their information private. . . .
 23 At the time, I invited you and the CEO of Twitter to participate in the hearing to
 24 discuss the future of data privacy in the social media industry. . . . ***Your office,
 25 however, declined to come before Congress and the American people, asserting
 26 that the problems surrounding Facebook and Cambridge Analytica did not
 27 involve Google.***

28 Given your and Google's unwillingness to participate. I sent you a letter seeking
 29 information on Google's current data privacy policies, specifically as they relate

23 Senator Blumenthal's Letter to FTC Chairman (October 10, 2018), available at <https://www.blumenthal.senate.gov/imo/media/doc/10.10.18%20-%20FTC%20-%20Google%20Plus%20Exposure.pdf> (last visited December 11, 2018); Senator Thune's Letter to Sundar Pichai (October 11, 2018), available at https://www.commerce.senate.gov/public/_cache/files/4852b311-0953-4ac8-ac43-a91dde229cc1/E300DA0C7659678AE0AE37AEB9746200.thune-wicker-moran-letter-to-google-10.11.18.pdf (last visited December 11, 2018); Senator Grassley's Letter to Sundar Pichai (October 11, 2018), available at <https://www.judiciary.senate.gov/imo/media/doc/2018-04-10%20CEG%20to%20Google%20-%20Data%20Privacy.pdf> (last visited December 11, 2018).

24 Senator Thune's Letter to Sundar Pichai, *supra* fn. 22.

1 to Google's third-party developer APIs. Your responses to my questions
 2 highlighted Google's application verification process, the continuous, monitoring
 3 of applications through machine learning, and the use of manual audits, all to
 ensure robust protection of user data.

4 *Despite your contention that Google did not have the same data protection*
 5 *failures as Facebook, it appears from recent reports that Google+ had an*
6 almost identical feature to Facebook, which allowed third party developers to
7 access information from users as well as private information of those users'
connections. Moreover, it appears that you were aware of this issue at the time I
 invited you to participate in the hearing and sent you the letter regarding
 Google's policies.²⁵

8 43. Defendant thus chose to protect itself from potential governmental inquiry rather
 9 than protect the Personal Information of Google+ users and advise them that their Personal
 10 Information had been exposed in the First Data Leak to unauthorized third parties.

11 44. Defendant withheld the information of the First Data Leak from Google+ users
 12 and the public until announcing it alongside its decision to shut down the Google+ service for
 13 consumers in August 2019 —approximately 10 months later.

14 45. At every turn, Defendant put its own business interests ahead of the privacy
 15 interests of Google+ users, causing harm to Plaintiffs and Class Members.

16 46. The First Data Leak has caused significant harm to Plaintiffs and other Class
 17 Members by allowing third-parties to access their Personal Information without their consent.
 18 This harm was exacerbated by Google's culture of concealment and opacity regarding its
 19 insufficient data protection policies and the resulting data breach.

20 47. Despite numerous lapses in and rebukes on its approach to data security, Google
 21 still lacks sufficient safeguards and protections for Users' Personal Information and has shown a
 22 conscious disregard for any transparency regarding the potential exposure of their personal
 23 information. This danger has already manifested in the Second Data Leak revealed by
 24 Defendant just months later. Thus, Plaintiffs and Class Members' Personal Information remains
 25 at risk today and into the future, until Google is compelled to secure their Personal Information.

26
 27
 28 ²⁵ Senator Grassley's Letter to Pichai, *supra* fn. 22 (emphasis added).

D. Defendant Failed to Properly Secure Google+ After the First Data Leak, Resulting in the Exposure of Even More Users' Personal Information in the Second Data Leak

48. Despite the increased attention from the First Data Leak in October 2018, Defendant continued to operate the Google+ service and collect Users' Personal Information, with no plans to shut the Google+ service down until August 2019.

49. Then, just *nine weeks* after their announcement of the First Data Leak, Defendant had to disclose that it had again improperly exposed Users' Personal Information to third-party application developers.

50. Specifically, on December 10, 2018, Defendant announced that it would be expediting its closure of Google+ due to the Second Data Leak, whereby the Personal Information of Users was, again, improperly exposed to third-party application developers.²⁶ This time, at least 52.5 million Users were impacted.²⁷ Defendant had permitted the Second Data Leak to persist from November 7, 2018 until November 13, 2018, when it allegedly identified and fixed vulnerabilities that had again permitted unauthorized third parties to access and aggregate Users' Personal Information.²⁸

51. The Second Data Leak allowed third-party application developers to view profile information from Users, including, *inter alia*, a User’s name, email address, occupation, work history, age, relationship status, biography, gender, and birthday – even if the User’s account was set to private.²⁹ Third-party developers were also able to improperly access Users’ profile data that had been shared with a specific User, but was not shared publicly by the User.³⁰

²⁶ Google, *Expediting changes to Google+* (December 10, 2018), available at <https://www.blog.google/technology/safety-security/expediting-changes-google-plus/> (last visited December 11, 2018).

²⁷ *Id.*
²⁸ Statt and Brandom, *Google will shut down Google+ four months early after second data leak* (December 10, 2018), available at <https://www.theverge.com/platform/amp/2018/12/10/18134541/google-plus-privacy-api-data-leakdevelopers> (last visited December 11, 2018).

²⁹ Google, *Expediting changes to Google*, *supra* fn. 25; Google, *Google+ API, List of Personal Information*, available at <https://developers.google.com/+/web/api/rest/latest/people> (last visited December 11, 2018). See also Statton and Brandom, *supra*, fn. 26.

30 *Id.*

1 52. As a result of the Second Data Leak, Defendant announced its decision to
 2 accelerate the shut-down of the consumer functionality of Google+ from August 2019 to April
 3 2019.³¹

4 **E. Users' Personal Information Is an Increasingly Valuable Commodity**

5 53. Personal information from social media, like the Personal Information
 6 encompassed in the Google+ Data Leaks, is incredibly valuable to companies like Google. In
 7 2017 alone, Google's advertisement revenue – which is dependent on Google's ability to collect
 8 personal information about its users – amounted to nearly \$95.4 billion.³²

9 54. One study found that the average consumer in the U.S. can make \$240 per year
 10 monetizing his or her personal data for digital advertising.³³ Another study in 2018 found that
 11 social media advertising revenue currently amounts to \$67.97 billion, and that the average
 12 revenue per Internet user currently amounts to approximately \$22.84.³⁴ Similarly, a 2016 study
 13 found that Google makes approximately \$7.00 per monthly active user each quarter, or
 14 approximately \$28.00 per user each year.³⁵

15 55. Defendant's calculation of the average revenue each user generates is derived
 16 from an analysis of, *inter alia*, the content and information each user shares.³⁶ Thus, when Users
 17 signed up to join Google+, they were entering into a transaction – a value-for-value exchange –
 18 in which they agreed to provide content and Personal Information that Defendant could use,
 19 subject to the Users' privacy restrictions. Because exclusive access to such content and

20

21

22

³¹ Google, *Expediting changes to Google*, *supra* fn. 25.

³² Alphabet, *Form 10-K* for the fiscal year ended December 31, 2017, filed with the SEC on February 6, 2018, at 28.

³³ Medium, *How Much is Your Data Worth? At Least \$240 per Year. Likely Much More*, available at <https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa> (last visited December 11, 2018).

³⁴ Statista, *Social Media Advertising*, available at <https://www.statista.com/outlook/220/100/social-media-advertising/worldwide#market-revenuePerInternetUser> (last visited December 11, 2018).

³⁵ Ampere Analysis, *Facebook Closes the Gap on Google*, available at <https://www.ampereanalysis.com/blog/fd5b6dc9-d76e-40a8-b8f2-e5ed15bc32bb> (last visited December 11, 2018).

³⁶ See, i.e., Google, *Google AdMob ARPU (metric)*, available at <https://support.google.com/admob/answer/7374260?hl=en> (discussing the metric of average revenue per user, or ABPU, that third-party application developers have access to when using Google's AdMob advertising platform).

1 information confers a competitive advantage, there is a “first user” value to the content and
 2 information. That value has now been lost due to the Google+ Data Leaks.

3 56. Additionally, the Personal Information compromised in the Google+ Data Leaks
 4 is highly valuable to identity thieves. The names, birthdates, hometowns, addresses, locations,
 5 interests, relationships, email addresses, photos, and videos, and other valuable personal
 6 information can all be used to gain access to a variety of existing accounts and websites.

7 57. Identity thieves can also use the Personal Information to harm Plaintiffs and the
 8 other Class Members through embarrassment, blackmail, or harassment in person or online or to
 9 commit other types of fraud including obtaining ID cards or driver’s licenses, fraudulently
 10 obtaining tax returns and refunds, and obtaining government benefits. A Presidential identity
 11 theft report from 2008 states that:

12 In addition to the losses that result when identity thieves fraudulently open
 13 accounts or misuse existing accounts, . . . individual victims often suffer indirect
 14 financial costs, including the costs incurred in both civil litigation initiated by
 15 creditors and in overcoming the many obstacles they face in obtaining or
 16 retaining credit. Victims of non-financial identity theft, for example, health-
 17 related or criminal record fraud, face other types of harm and frustration.

18 In addition to out-of-pocket expenses that can reach thousands of dollars for the
 19 victims of new account identity theft, and the emotional toll identity theft can
 20 take, some victims have to spend what can be a considerable amount of time to
 21 repair the damage caused by the identity thieves. Victims of new account identity
 22 theft, for example, must correct fraudulent information in their credit reports and
 23 monitor their reports for future inaccuracies, close existing bank accounts and
 24 open new ones, and dispute charges with individual creditors.³⁷

25 58. To put it into context, the 2013 Norton Report³⁸ – based on one of the largest
 26 consumer cybercrime studies ever conducted – estimated that the global price tag of cybercrime
 27 was around **\$113 billion** at that time, with the average cost per victim being \$298 dollars, as
 28 demonstrated in the chart below:

26 37 U.S. FTC, *The President’s Identity Theft Task Force, Combating Identity Theft: A Strategic Plan*, (April
 27 2007), <https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf> (last visited December 11, 2018).

28 38 Norton by Symantec, *2013 Norton Report*, available at
https://yle.fi/tvuutiset/uutiset/upics/tilitiedostot/norton_raportti.pdf (last visited December 10, 2018).



59. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the Personal Information they have obtained. Indeed, in order to protect themselves, Plaintiffs and the other Class Members will need to remain vigilant against unauthorized data use for years and decades to come.

60. Once stolen, personal information can be used in a number of different ways. One of the most common ways is that it is offered for sale on the dark web, a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. Due to its hidden nature and the use of special applications to maintain anonymity, the dark web is a haven for all kinds of illicit activity, including the trafficking of stolen personal information captured via data breaches or hacks.³⁹ One 2018 study found that an individual's online identity is worth approximately \$1,170 on the dark web.⁴⁰

³⁹ Experian, *What is the Dark Web?* (April 8, 2018), available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/> (last visited December 10, 2018). See also Brian Hamrick, *The dark web: A trip into the underbelly of the internet*, WLWT News (Feb. 9, 2017), <http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419> (last visited December 10, 2018).

⁴⁰ TOP10VPN, Dark Web Market Price Index (US Edition) (February 27, 2018), available at <https://www.top10vpn.com/privacy-central/privacy/dark-web-market-price-index-feb-2018-us/> (last visited December 10, 2018).

1 61. Once someone buys personal information, it is then used to gain access to
 2 different areas of the victim's digital life, including bank accounts, social media, and credit card
 3 details. During that process, other sensitive data may be harvested from the victim's accounts,
 4 as well as from those belonging to family, friends, and colleagues.

5 62. Personal information can also be used by scammers to target victims using
 6 phishing scams.⁴¹ Phishing is when scammers use personal information they have obtained
 7 about victims to send fraudulent emails or texts, or copycat websites to get victims to share
 8 additional valuable personal information – such as account numbers, Social Security numbers,
 9 or login IDs and passwords.⁴² Scammers use victims' information, including Personal
 10 Information, to steal the victims' money, identity, or both.⁴³ Scammers also use phishing emails
 11 to get access to a victim's computer or network, then install programs like ransomware that can
 12 lock a victim out of important files on their computer.⁴⁴ According to one Federal Bureau of
 13 Investigation study, scammers collected more than \$676 million in 2017 alone through two
 14 types of phishing scams: "Business Email Compromise" and "Email Account Compromise."⁴⁵

15 63. Due to Defendant's conduct described herein, Plaintiffs and the other Class
 16 Members have a greater risk of identity theft, manipulation, fraud, scams, and/or targeted
 17 unwanted and unnecessary advertising, including inappropriate communications. Additionally,
 18 Plaintiffs and the other Class Members now face additional security risks such as phishing
 19 attempts, efforts by hackers trying to access or log in to their online accounts, friend requests
 20 from trolls or cloned or imposter accounts, and/or other interference with their online accounts.

21

⁴¹ U.S. FTC, *Phishing* (July 2017), available at <https://www.consumer.ftc.gov/articles/0003-phishing> (last visited December 12, 2018).

22 ⁴² *Id.*

23 ⁴³ *Id.*

24 ⁴⁴ *Id.*

25 ⁴⁵ U.S. Federal Bureau of Investigation, *2017 Internet Crime Report*, available at
 26 https://pdf.ic3.gov/2017_IC3Report.pdf (last visited December 12, 2018).

1 Plaintiffs and the other Class Members are subjected to a heightened risk of such predatory
 2 conduct due to Defendant's failure to secure their Personal Information, including the sale of
 3 their content and Personal Information on the dark web and other illicit databases.

4 **F. Google Has A Long History of Improper Data Practices**

5 64. Google has been on notice of deficiencies regarding its policies involving the
 6 retention of User data since at least 2010. The FTC specifically found that Google used
 7 deceptive tactics and violated its own privacy promises to consumers when it launched its first
 8 social network product, Google Buzz, in 2010.

9 65. As a result of such deficiencies, Google agreed to a proposed settlement in
 10 March 2011, which contained a consent decree under which the FTC barred Google from
 11 misrepresenting the privacy of personal information or the extent to which consumers may
 12 exercise control over the collection, use, or exposure of their covered personal information.⁴⁶
 13 The FTC also required Google to establish a "comprehensive privacy program that is
 14 reasonably designed to: (1) address privacy risks related to the development and management of
 15 new and existing products and services for consumers, and (2) protect the privacy and
 16 confidentiality of covered information." Included in this privacy program was the "regular
 17 testing or monitoring of the effectiveness of those privacy controls and procedures," which
 18 would be audited by an independent third-party professional.⁴⁷

19 66. Less than a year after entering into the FTC consent decree, Google violated it –
 20 becoming one of the rare companies in the country that has violated an FTC consent decree –
 21 and paid a record fine for its circumvention of privacy protections in the web browser Safari.⁴⁸
 22

23
 24 _____
 25 ⁴⁶ U.S. FTC, *In the Matter of GOOGLE INC., a corporation* (October 13, 2011), Docket No. C-4436,
 26 available at <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf> (last visited
 27 December 11, 2018).

28 ⁴⁷ *Id.*

⁴⁸ U.S. FTC, *Google Will Pay \$22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (August 9, 2012), available at <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> (last visited December 11, 2018).

1 In discussing the settlement, Jon Leibowitz, Chairman of the FTC, said, “The record setting
 2 penalty in this matter sends a clear message to all companies under an FTC privacy order. No
 3 matter how big or small, all companies must abide by FTC orders against them and keep their
 4 privacy promises to consumers, or they will end up paying many times what it would have cost
 5 to comply in the first place.”⁴⁹

6 **PLAINTIFFS’ FACTUAL ALLEGATIONS**

7 **A. Plaintiff Matt Matic**

8 67. Plaintiff Matt Matic is a resident and citizen of the state of California.

9 68. Mr. Matic uses Gmail as his primary email account.

10 69. Mr. Matic has had and actively used his Google+ account since 2014.

11 70. Mr. Matic provided Defendant with Personal Information, including his name,
 12 birthdate, gender, email address, mailing address, cellular telephone number, multiple credit
 13 card numbers with expiration dates and corresponding billing addresses, and the makes and
 14 models of the smart devices he owns and uses to access his Google+ account.

15 71. Mr. Matic also stored contact information for multiple personal contacts in his
 16 Google+ account, including the contacts’ names and cellular telephone numbers.

17 72. Additionally, Mr. Matic stored and managed passwords for 14 non-Google
 18 online accounts within his Google+ account, including Amazon.com, AOL.com,
 19 BankofAmerica.com, Blockchain.com, Chess.com, ClubWPT.com, eSmartTax.com,
 20 Facebook.com, FocusGroups.org, Groupon.com, iFleet.com, Media-Services.com, and
 21 PapaJohns.com.

22 73. Mr. Matic made more than 20 online purchases via his Google+ account, which
 23 maintained detailed purchase transaction records dating back to 2014, including payment card
 24 details.

25 74. Mr. Matic’s Google+ account contains detailed records of his web and app
 26 activity, as well as his YouTube search and viewing histories.

27

28

⁴⁹ *Id.*

1 75. Mr. Matic's Google+ account also contains his location history, which includes
 2 detailed records of more than 320 locations that he has visited over the past several years.

3 76. Mr. Matic's Google+ account enabled certain third-party applications to access
 4 his Google+ account and data, Google Drive, and Google Contacts. Although Mr. Matic
 5 permitted certain third-party applications to access his Google+ account and data, Mr. Matic
 6 limited that access to these third-party application developers and chose not to permit every
 7 single third-party application developer to access his Google+ account and data.

8 77. Mr. Matic has consistently monitored and maintained his Google+ account
 9 security settings and regularly changed his password. He most recently changed his password in
 10 September 2018.

11 78. On October 8, 2018, Defendant belatedly announced its First Data Leak, and on
 12 December 10, 2018, Defendant announced its Second Data Leak. Through these
 13 announcements, Mr. Matic discovered that Defendant had improperly exposed his Personal
 14 Information and the additional private and sensitive data described above to unauthorized third-
 15 party application developers.

16 79. As a result of Google's Data Leaks, Mr. Matic suffered exposure of what had
 17 been a tightly maintained and secure Google+ account, including Personal Information as well
 18 as the additional private and sensitive data described above.

19 **B. Plaintiff Zak Harris**

20 80. Plaintiff Zak Harris is a resident and citizen of the state of Florida.

21 81. Mr. Harris uses Gmail as his primary email account.

22 82. Mr. Harris has had and actively used his Google+ account since 2011.

23 83. Mr. Harris provided Defendant with Personal Information, including his name,
 24 birthdate, gender, email address, mailing address, cellular telephone number, high school name,
 25 place of employment, personal photos and videos, multiple credit card numbers with expiration
 26 dates and corresponding billing addresses, Paypal account details, and the makes and models of
 27 the smart devices he owns and uses to access his Google+ account.

1 84. Mr. Harris also stored contact information for more than 50 personal contacts in
 2 his Google+ account, including the contacts' names and email addresses.

3 85. Mr. Harris made more than 70 online purchases and money transfers via his
 4 Google+ account, which maintained detailed purchase transaction records dating back to 2011.

5 86. Mr. Harris also made more than 160 purchases from online retailers such as
 6 Amazon.com, BestBuy.com, NewEgg.com via his Google+ account, which maintained detailed
 7 purchase transaction records, including his Amazon search history, purchase history, and
 8 payment card details and corresponding billing and mailing addresses, dating back to 2013.

9 87. Mr. Harris's Google+ account contains detailed records of his web and app
 10 activity, as well as his Internet search history, and YouTube search and viewing histories.

11 88. Mr. Harris has consistently monitored and maintained his Google+ account
 12 security settings and regularly changed his password.

13 89. On October 8, 2018, Defendant belatedly announced its First Data Leak, and on
 14 December 10, 2018, Defendant announced its Second Data Leak. Through these
 15 announcements, Mr. Harris discovered that Defendant had improperly exposed his Personal
 16 Information and the additional private and sensitive data described above to third-party
 17 application developers.

18 90. As a result of Google's Data Leaks, Mr. Harris suffered exposure of what had
 19 been a tightly maintained and secure Google+ account, including Personal Information as well
 20 as the additional private and sensitive data described above.

21 **C. Plaintiff Charles Olson**

22 91. Plaintiff Charles Olson is a resident and citizen of the state of Colorado.

23 92. Mr. Olson uses Gmail as his primary email account.

24 93. Mr. Olson has had and actively used his Google+ account since 2014.

25 94. Mr. Olson provided Defendant with Personal Information, including his name,
 26 birthdate, gender, email address, mailing address, telephone numbers, place of employment,
 27 location, interests, personal photos and videos, multiple credit card numbers with expiration

1 dates and corresponding billing addresses, checking account numbers, and the makes and
 2 models of the smart devices he owns and uses to access his Google+ account.

3 95. Mr. Olson also stored contact information for multiple personal contacts in his
 4 Google+ account, including the contacts' names, email addresses and cellular telephone
 5 numbers.

6 96. Additionally, Mr. Olson stored and managed passwords for multiple non-Google
 7 online accounts within his Google+ account, including Facebook.com, Starbucks.com,
 8 GreenDot.com and WesternUnion.com.

9 97. Additionally, Mr. Olson used his Google+ account to text and chat with people
 10 in his circles. His account contains detailed text and chat logs of his personal and private
 11 conversations.

12 98. Mr. Olson's Google+ account contains detailed records of his web and app
 13 activity, as well as his Internet search history and website visits, and YouTube search and
 14 viewing histories.

15 99. Mr. Olson's Google+ account also contains his location history, which includes
 16 detailed records of more than 27 locations that he has visited over the past several years.

17 100. Mr. Olson's Google+ account enabled certain third-party applications to access
 18 his Google+ account and data. Although Mr. Olson permitted certain third-party applications to
 19 access his Google+ account and data, Mr. Olson limited that access to these third-party
 20 application developers and chose not to permit every single third-party application developer to
 21 access his Google+ account and data.

22 101. Mr. Olson has consistently monitored and maintained his Google+ account
 23 security settings and regularly changed his Google PIN and password. He last changed his PIN
 24 on October 25, 2018, and his password on October 27, 2018. Mr. Olson also installed security
 25 apps and anti-virus software on his computer.

26 102. On October 8, 2018, Defendant belatedly announced its First Data Leak, and on
 27 December 10, 2018, Defendant announced its Second Data Leak. Through these
 28 announcements, Mr. Olson discovered that Defendant had improperly exposed his Personal

1 Information and the additional private and sensitive data described above to unauthorized third-
 2 party application developers.

3 103. As a result of Google's Data Leaks, Mr. Olson suffered exposure of what had
 4 been a tightly maintained and secure Google+ account, including Personal Information as well
 5 as the additional private and sensitive data described above.

6 **D. Plaintiff Eileen M. Pinkowski**

7 104. Plaintiff Eileen M. Pinkowski is a resident and citizen of the state of Colorado.

8 105. Ms. Pinkowski has used Gmail as her primary email account.

9 106. Ms. Pinkowski has had and actively used her Google+ account since 2011.

10 107. Ms. Pinkowski provided Defendant with Personal Information, including her
 11 name, birthdate, gender, email address, mailing address, multiple telephone numbers,
 12 hometown, location, interests, relationship status, personal photos and videos.

13 108. Ms. Pinkowski also stored contact information for multiple personal contacts in
 14 her Google+ account, including the contacts' names and email addresses.

15 109. Ms. Pinkowski also made more than 40 in-app and online purchases from
 16 retailers such as iTunes and Wayfair.com via her Google+ account, which maintained detailed
 17 purchase transaction records.

18 110. Ms. Pinkowski's Google+ account contains detailed records of her web and app
 19 activity, as well as her ad viewing history, Internet search and shopping history, and YouTube
 20 search and viewing histories dating back to 2010.

21 111. Ms. Pinkowski has consistently monitored and maintained her Google+ account
 22 security settings and regularly changed her password, as well as opening new email accounts
 23 with unique names.

24 112. On October 8, 2018, Defendant belatedly announced its First Data Leak, and on
 25 December 10, 2018, Defendant announced its Second Data Leak. Through these
 26 announcements, Ms. Pinkowski discovered that Defendant had improperly exposed her Personal
 27 Information and the additional private and sensitive data described above to unauthorized third-
 28 party application developers.

113. As a result of Google's Data Leaks, Ms. Pinkowski suffered exposure of what had been a tightly maintained and secure Google+ account, including Personal Information as well as the additional private and sensitive data described above.

CLASS ACTION ALLEGATIONS

114. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3), and (c)(4), Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following Class:

All persons in the United States who registered for Google+ accounts and whose Personal Information was accessed, compromised, or obtained from Google by third-party applications without authorization or in excess of authorization as a result of the 2018 Data Leaks. (“Class”).

115. Excluded from the Class are Defendant and any entities in which Defendant or its subsidiaries or affiliates have a controlling interest, as well as Defendant's officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family. Plaintiffs reserve the right to amend the Class definitions if discovery and further investigation reveal that any definitions should be expanded or otherwise modified.

116. **Numerosity:** The Members of the Class are so numerous that joinder of all Members of the Class would be impracticable. Defendant has indicated that at least 500,000 people had their Google+ accounts compromised as a result of the First Data Leak, and as many as 52,500,000 people had their Google+ accounts compromised as a result of the Second Data Leak. The identity of these Google+ users can be determined through records and documents maintained by Defendant.

117. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class Members, including:

- i. Whether Defendant represented to Plaintiffs and the Class that it would safeguard Class Members' Personal Information;
- ii. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

1 119. Google's choice-of-law provision is further indication of the common questions
 2 of law. Google's Terms of Service provide, in relevant part, that "you agree that the laws of
 3 California, U.S.A., excluding California's choice of law rules, will apply to any disputes arising
 4 out of or relating to these terms or the Services."

5 120. **Typicality:** Plaintiffs' claims are typical of the claims of the other Members of
 6 the Class because, among other things, Plaintiffs and the other Class Members were injured
 7 through the substantially uniform misconduct by Defendant. Plaintiffs are advancing the same
 8 claims and legal theories on behalf of themselves and all other Class Members, and there are no
 9 defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class Members
 10 arise from the same operative facts and are based on the same legal theories.

11 121. **Adequacy of Representation:** Plaintiffs are adequate representatives of the
 12 Class because their interests do not conflict with the interests of the other Class Members they
 13 seek to represent, they have retained counsel competent and experienced in complex class
 14 action litigation, and they will prosecute this action vigorously. The Class Members' interests
 15 will be fairly and adequately protected by Plaintiffs and their counsel.

16 122. **Superiority:** A class action is superior to any other available means for the fair
 17 and efficient adjudication of this controversy, and no unusual difficulties are likely to be
 18 encountered in the management of this matter as a class action. The damages, harm, or other
 19 financial detriment suffered individually by Plaintiffs and the other Members of the Class are
 20 relatively small compared to the burden and expense that would be required to litigate their
 21 claims on an individual basis against Defendant, making it impracticable for Class Members to
 22 individually seek redress for Defendant's wrongful conduct. Even if Class Members could
 23 afford individual litigation, the court system could not. Individualized litigation would create a
 24 potential for inconsistent or contradictory judgments, and increase the delay and expense to all
 25 parties and the court system. By contrast, the class action device presents far fewer management
 26 difficulties and provides the benefits of single adjudication, economies of scale, and
 27 comprehensive supervision by a single court.

28

1 123. Further, Defendant has acted or refused to act on grounds generally applicable to
 2 the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to
 3 the Members of the Class as a whole is appropriate under Rule 23(b)(2).

4 124. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification
 5 because such claims present only particular, common issues, the resolution of which would
 6 advance the disposition of this matter and the parties' interests therein. Such particular issues
 7 include, but are not limited to:

- 8 a. Whether Class Members' Personal Information was improperly obtained by third
 9 parties;
- 10 b. Whether (and when) Defendant knew about any security vulnerabilities that led
 11 to the First Data Leak before they were announced to the public and whether
 12 Defendant failed to timely notify the public of those vulnerabilities and the First
 13 Data Leak;
- 14 c. Whether (and when) Defendant knew about any security vulnerabilities that led
 15 to the Second Data Leak before they were announced to the public and whether
 16 Defendant failed to timely notify the public of those vulnerabilities and the Second
 17 Data Leak;
- 18 d. Whether Defendant's conduct was an unlawful or unfair business practice under
 19 Cal. Bus. & Prof. Code § 17200, *et seq.*;
- 20 e. Whether Defendant's representations that it would secure and protect the
 21 Personal Information of Plaintiffs and the other Members of the Class were facts
 22 that reasonable persons could be expected to rely upon when deciding whether to
 23 use Defendant's services;
- 24 f. Whether Defendant misrepresented the safety of its many systems and services,
 25 specifically the security thereof, and its ability to safely store Plaintiffs' and the
 26 other Class Members' Personal Information;
- 27 g. Whether Defendant concealed crucial information about its inadequate data
 28 security measures from Plaintiffs and the Class;
- 29 h. Whether Defendant failed to comply with its own policies and applicable laws,
 30 regulations, and industry standards relating to data security;
- 31 i. Whether Defendant knew or should have known that it did not employ
 32 reasonable measures to keep Plaintiffs' and the other Class Members' Personal
 33 Information secure and prevent the unauthorized disclosure of that information;

- j. Whether Defendant failed to “implement and maintain reasonable security procedures and practices” for Plaintiffs’ and the other Class Members’ Personal Information in violation of § 5 of the FTC Act;
- k. Whether Defendant failed to provide timely notice of the First Data Leak in violation of California Civil Code § 1798.82;
- l. Whether Defendant failed to provide timely notice of the Second Data Leak in violation of California Civil Code § 1798.82;
- m. Whether Defendant’s conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.*;
- n. Whether Defendant owed a duty to Plaintiffs and the Class to safeguard their Personal Information and to implement adequate data security measures;
- o. Whether Defendant breached that duty;
- p. Whether Defendant failed to adhere to its posted privacy policy concerning the care they would take to safeguard Plaintiffs’ and the other Class Members’ Personal Information in violation of California Business and Professions Code § 22576;
- q. Whether Defendant negligently and materially failed to adhere to its posted privacy policy with respect to the extent of its disclosure of users’ data, in violation of California Business and Professions Code § 22576;
- r. Whether such representations were false with regard to storing and safeguarding Class and Class Members’ Personal Information; and
- s. Whether such representations were material with regard to storing and safeguarding Class Members’ Personal Information.

First Claim for Relief

Violation of California's Unfair Competition Law ("UCL") – Unlawful Business Practice (Cal. Bus. & Prof. Code § 17200, *et seq.*)

125. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained in Paragraphs 1 through 124 as though the same were fully set forth herein.

126. Defendant's choice-of-law provision establishes that California law applies to Plaintiffs' and the other Class Members' claims.

127. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a “business practice” within the meaning of the UCL.

1 128. Google represented that it would not disclose Google+ users' Personal
 2 Information without consent and/or notice. Google further represented that it would utilize
 3 sufficient data security protocols and mechanisms to protect Google+ users' Personal
 4 Information.

5 129. Defendant failed to abide by these representations. Defendant did not prevent the
 6 improper disclosure of Plaintiffs' and the Class's Personal Information.

7 130. Defendant stored the Personal Information of Plaintiffs and the Members of the
 8 Class in Defendant's electronic and consumer information databases. Defendant falsely
 9 represented to Plaintiffs and the other Members of the Class that the Personal Information
 10 databases were secure and that their Personal Information would remain private. Defendant
 11 knew or should have known it did not employ reasonable, industry standard, and appropriate
 12 security measures that complied "with federal regulations" and that would have kept Plaintiffs'
 13 and the other Class Members' Personal Information secure and prevented the loss or misuse of
 14 such Personal Information.

15 131. Even without these misrepresentations, Plaintiffs and the other Class Members
 16 were entitled to assume, and did assume, that Defendant would take appropriate measures to
 17 keep their Personal Information safe. Defendant did not disclose at any time that Plaintiffs'
 18 Personal Information was accessible to third party application vendors because Defendant's
 19 data security measures were inadequate, even though Defendant was the only one in possession
 20 of that material information, which it had a duty to disclose. Defendant violated the UCL by
 21 misrepresenting, both by affirmative conduct and by omission, the strength of the security of its
 22 many systems and services, and its ability to honor the disclosure authorizations established by
 23 Plaintiffs and the other Class Members for their Personal Information.

24 132. Defendant also violated the UCL by failing to implement reasonable and
 25 appropriate security measures or follow industry standards for data security, and failing to
 26 comply with its own posted privacy policies. If Defendant had complied with these legal
 27 requirements, Plaintiffs and the other Class Members would not have suffered the damages
 28 described herein.

133. Defendant's acts, omissions, and misrepresentations, as alleged herein, were unlawful and in violation of, *inter alia*, Section 5(a) of the FTC Act and 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (as a result of Google failing to comply with its own posted privacy policies).

134. Plaintiffs and the other Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In particular, Plaintiffs' and the other Class Members' Personal Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that such information is of tangible value.

135. As a result of Defendant's unlawful business practices, which are violations of the UCL, Plaintiffs and the other Class Members are entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

Second Claim for Relief
Violation of California's UCL – Unfair Business Practice
(Cal. Bus. & Prof. Code § 17200, *et seq.*)

136. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained in Paragraphs 1 through 124 as though the same were fully set forth herein.

137. Defendant's choice-of-law provision establishes that California law applies to Plaintiffs' and the other Class Members' claims.

138. By reason of the conduct alleged herein, Defendant engaged in unfair “business practices” within the meaning of the UCL.

139. Defendant stored the Personal Information of Plaintiffs and the Members of the Class in its electronic and consumer information databases. Defendant represented to Plaintiffs and the other Members of the Class that its Personal Information databases were secure and that such Personal Information would remain private and be disclosed only with expressed authorization. Defendant engaged in unfair acts and business practices by representing that it would require expressed consent and authorization from Plaintiffs and the other Class Members prior to the disclosure of Personal Information to third parties.

1 140. Even without these misrepresentations, Plaintiffs and the other Class Members
 2 were entitled to, and did, assume Defendant would take appropriate measures to keep their
 3 Personal Information safe. Defendant did not disclose at any time that Plaintiffs' Personal
 4 Information was vulnerable to unauthorized disclosure because Defendant's data security
 5 measures were inadequate, even though Defendant was in sole possession of that material
 6 information, which it had a duty to disclose.

7 141. Defendant knew or should have known it did not employ reasonable measures
 8 that would have kept Plaintiffs' and the other Class Members' Personal Information secure from
 9 unauthorized disclosure.

10 142. Defendant engaged in unfair acts and business practices by representing that it
 11 would not disclose this Personal Information without authorization and/or by obtaining that
 12 Personal Information without authorization. Not only did Defendant violate its commitment to
 13 maintain the confidentiality and security of the Personal Information of Plaintiffs and the Class,
 14 but it failed to comply with its own stated policies and applicable laws, regulations, and industry
 15 standards relating to data security.

16 143. **Defendant engaged in unfair business practices under the "balancing test."**
 17 The harm caused by Defendant's actions and omissions, as described in detail *supra*, greatly
 18 outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security
 19 protocols and misrepresentations to consumers about Defendant's data security cannot be said
 20 to have had any utility at all.

21 144. **Defendant engaged in unfair business practices under the "tethering test."**
 22 Defendant's actions and omissions, as described in detail *supra*, violated fundamental public
 23 policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The
 24 Legislature declares that ... all individuals have a right of privacy in information pertaining to
 25 them.... The increasing use of computers ... has greatly magnified the potential risk to individual
 26 privacy that can occur from the maintenance of Personal Information."); Cal. Bus. & Prof. Code
 27 § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy
 28 Protection Act] is a matter of statewide concern."). Defendant's acts and omissions, and the

1 injuries caused by them, are thus “comparable to or the same as a violation of the law ...” *Cel-*
 2 *Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

3 145. **Defendant engaged in unfair business practices under the “FTC test.”** The
 4 harm caused by Defendant’s actions and omissions, as described in detail *supra*, is substantial in
 5 that it affects at least 53 million Class Members and has caused those persons to suffer actual
 6 harms. Such harms include a substantial risk of identity theft, disclosure of Class Members’
 7 Personal Information to third parties without their consent, diminution in value of their Personal
 8 Information, and consequential out-of-pocket losses for procuring credit freeze or protection
 9 services, identity theft monitoring, and other expenses relating to identity theft losses or
 10 protective measures. This harm continues given the fact that Class Members’ Personal
 11 Information remains in Defendant’s possession, without adequate protection, and is also in the
 12 hands of those who obtained it without their consent. Defendant’s actions and omissions
 13 violated, *inter alia*, Section 5(a) of the FTC Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham*
 14 *Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff’d*, 799 F.3d 236 (3d Cir. 2015); *In*
 15 *re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to
 16 employ reasonable and appropriate measures to secure Personal Information collected violated §
 17 5(a) of FTC Act); *In re BJ’s Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-
 18 3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC
 19 File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil
 20 Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) (“failure to establish and implement,
 21 and thereafter maintain, a comprehensive information security program that is reasonably
 22 designed to protect the security, confidentiality, and integrity of Personal Information collected
 23 from or about consumers” violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining “unfair acts
 24 or practices” as those that “cause[] or [are] likely to cause substantial injury to consumers which
 25 [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing
 26 benefits to consumers or to competition.”).

27 146. Plaintiffs and the other Class Members suffered injury in fact and lost money or
 28 property as the result of Defendant’s unfair business practices. In addition, their Personal

1 Information was taken and is in the hands of those who will use it for their own advantage, or is
 2 being sold for value, making it clear that the hacked information is of tangible value.

3 147. As a result of Defendant's unfair business practices, which are violations of the
 4 UCL, Plaintiffs and the other Class Members are entitled to restitution, disgorgement of
 5 wrongfully obtained profits, and injunctive relief.

6 **Third Claim for Relief**
 7 **Violation of California's UCL – Fraudulent/Deceptive Business Practice**
 8 **(Cal. Bus. & Prof. Code § 17200, *et seq.*)**

9 148. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every
 10 allegation contained in Paragraphs 1 through 124 as though the same were fully set forth herein.

11 149. Defendant's choice-of-law provision establishes that California law applies to
 12 Plaintiffs' and the other Class Members' claims.

13 150. Defendant engaged in fraudulent and deceptive acts and practices with regard to
 14 the services it provided to the Class by representing and advertising that (1) it would maintain
 15 adequate data privacy and security practices and procedures to safeguard Class Members'
 16 Personal Information from unauthorized disclosure, release, data breaches, and theft; and (2) it
 17 did and would comply with the requirements of relevant federal and state laws pertaining to the
 18 privacy and security of Class Members' Personal Information. These representations were likely
 19 to deceive members of the public, including Plaintiffs and the other Class Members, into
 20 believing their Personal Information was securely stored – when it was not – and that Defendant
 21 was complying with relevant law – when it was not.

22 151. Defendant engaged in fraudulent and deceptive acts and practices with regard to
 23 the services provided to the Class by omitting, suppressing, and concealing the material fact that
 24 the privacy and security protections for Class Members' Personal Information was woefully
 25 inadequate. At the time that Class Members were using Defendant's services, Defendant failed
 26 to disclose to Class Members that its data security systems failed to meet legal and industry
 27 standards for the protection of Class Members' Personal Information. These representations
 28 likely deceived members of the public, including Plaintiffs and the Class, into believing that

1 their Personal Information was securely stored – when it was not – and that Defendant was
 2 complying with relevant law and industry standards – when it was not.

3 152. As a direct and proximate result of Defendant's deceptive practices and acts,
 4 Plaintiffs and the Class were injured and lost money or property, including but not limited to the
 5 loss of their legally protected interest in the confidentiality and privacy of their Personal
 6 Information, as well as the additional losses described *supra*.

7 153. Defendant knew or should have known that its computer systems and data
 8 security practices were inadequately safeguarding Class Members' Personal Information and
 9 that the risk of a data breach or theft was very high.

10 154. Defendant's actions in engaging in the above-named unlawful practices and acts
 11 were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of
 12 Members of the Class.

13 155. Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq.*,
 14 including, but not limited to, restitution to Plaintiffs and the Class of money or property that
 15 Defendant may have acquired by means of its fraudulent and deceptive business practices,
 16 restitutionary disgorgement of all profits accruing to Defendant because of its fraudulent and
 17 deceptive business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code
 18 Civ. Proc. § 1021.5), and injunctive or other equitable relief.

19 **Fourth Claim for Relief**
 20 **Negligence**

21 156. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every
 22 allegation contained in Paragraphs 1 through 124 as though the same were fully set forth herein.

23 157. Defendant's choice-of-law provision establishes that California law applies to
 24 Plaintiffs' and all Class Members' claims.

25 158. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in
 26 safeguarding and protecting their Personal Information and keeping it from being compromised,
 27 lost, stolen, misused, and or/disclosed to unauthorized parties.

1 159. Defendant knew that the Personal Information of Plaintiffs and the Class was
 2 personal and sensitive information that is valuable to identity thieves and other criminals.
 3 Defendant also knew of the serious harms that could occur if the Personal Information of
 4 Plaintiffs and the Class was wrongfully disclosed, that disclosure was not fixed, and/or
 5 Plaintiffs and the Class were not told about the disclosure in a timely manner.

6 160. By being entrusted by Plaintiffs and the Class to safeguard their Personal
 7 Information, Defendant had a special relationship with Plaintiffs and the Class. Plaintiffs and
 8 the Class signed up for Defendant's services and agreed to provide their Personal Information
 9 with the understanding that Defendant would take appropriate measures to protect it and would
 10 inform Plaintiffs and the Class of any breaches or other security concerns that might call for
 11 action by Plaintiffs and the Class. But, Defendant did not. Defendant not only knew that its data
 12 security was inadequate, it also knew that it did not have the tools to detect and document
 13 intrusions or exfiltration of Plaintiffs' and the Class' Personal Information.

14 161. Defendant breached its duty to exercise reasonable care in safeguarding and
 15 protecting Plaintiffs' and the Class Members' Personal Information by failing to adopt,
 16 implement, and maintain adequate security measures to safeguard that information and prevent
 17 unauthorized disclosure of Plaintiffs' and the other Class Members' Personal Information.

18 162. Defendant also breached its duty to timely disclose that Plaintiffs' and the other
 19 Class Members' Personal Information had been, or was reasonably believed to have been,
 20 improperly obtained.

21 163. But for Defendant's wrongful and negligent breach of its duties owed to
 22 Plaintiffs and the Class, their Personal Information would not have been compromised, stolen,
 23 and viewed by unauthorized persons.

24 164. Defendant's negligence was a direct and legal cause of the theft of the Personal
 25 Information of Plaintiffs and the Class and all resulting damages.

26 165. The injury and harm suffered by Plaintiffs and the other Class Members was the
 27 reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding
 28 and protecting Plaintiffs' and the other Class Members' Personal Information. Defendant knew

1 its systems and technologies for processing and securing the Personal Information of Plaintiffs
 2 and the Class had numerous security vulnerabilities.

3 166. As a result of this misconduct by Defendant, the Personal Information of
 4 Plaintiffs and the Class was compromised – placing them at a greater risk of identity theft and
 5 subjecting them to identity theft – and was disclosed to third parties without their consent.

6 167. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and
 7 the other Class Members have suffered injury and are entitled to appropriate relief, including
 8 injunctive relief and damages.

9 **Fifth Claim for Relief**
 10 **Invasion of Privacy**

11 168. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every
 12 allegation contained in Paragraphs 1 through 124 as though the same were fully set forth herein.

13 169. Defendant's choice-of-law provision establishes that California law applies to
 14 Plaintiffs' and all Class Members' claims.

15 170. The California Constitution expressly provides for a right to privacy. Cal. Const.
 16 Art. I, Sec. 1.

17 171. Google's terms of use for all times relevant to this matter provided that users'
 18 Personal Information would not be released to third parties without express consent.

19 172. Absent their express consent, Plaintiffs and the other Class Members used
 20 Google+ under the impression that Personal Information was safeguarded and would not be
 21 provided to, or stolen by, third parties.

22 173. Plaintiffs and the other Class Members had an interest in the protection and non-
 23 dissemination of their Personal Information that Defendant electronically stored, including the
 24 right not to have that Personal Information stolen and used for profit.

25 174. Absent the express consent of Google+ users, Defendant intentionally intruded
 26 on Plaintiffs' and the other Class Members' private life, seclusion, and solitude, which is
 27 protected under the California constitution as well as common law.

175. Defendant's wrongful conduct constitutes breach of the social norms underpinning the constitutionally-protected right to privacy.

176. Defendant's wrongful conduct harmed Plaintiffs and the other Class Members.

177. As a direct and proximate result of Defendant's wrongful conduct, Plaintiffs and the other Class Members have suffered injury and are entitled to appropriate relief, including injunctive relief and damages.

Sixth Claim for Relief
Breach of Confidence

178. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained in Paragraphs 1 through 124 as though the same were fully set forth herein.

179. This claim is asserted against Defendant for breach of confidence concerning the Personal Information that Plaintiffs and the other Class Members provided to Defendant in confidence

180. At all times during Plaintiffs' and the other Class Members' interactions with Defendant, Defendant was fully aware of the confidential nature of the Personal Information that Plaintiffs and Class Members shared with Defendant

181. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by Google's Terms of Service and the expectation that Plaintiffs' and Class Members' Personal Information would be collected, stored, and protected in confidence by Defendant, and not disclosed to unauthorized third parties.

182. Plaintiffs and the other Class Members provided their respective Personal Information to Defendant with the explicit and implicit understanding that Defendant would protect and not permit that Personal Information to be disseminated to any unauthorized third parties.

183. Defendant voluntarily received in confidence Plaintiffs' and the other Class Members' Personal Information with the understanding that that Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

1 184. Due to Defendant's failure to prevent, detect, and stop the 2018 Data Leaks from
2 occurring, Plaintiffs' and the other Class Members' Personal Information was disclosed and
3 misappropriated to unauthorized third parties beyond their confidence and without their express
4 permission.

5 185. As a direct and proximate cause of Defendant's actions and inactions, Plaintiffs
6 and the other Class Members have suffered damages.

7 186. But for Defendant's disclosure of Personal Information in violation of the
8 parties' understanding that it would be held in confidence, Plaintiffs and the other Class
9 Members' Personal Information would not have been compromised, stolen, and viewed by
10 unauthorized persons. Defendant's disclosure was a direct and legal cause of the theft of
11 Plaintiffs' and the other Class Members' Personal Information, as well as the resulting damages.

12 187. The injury and harm Plaintiffs and the other Class Members suffered was the
13 reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class
14 Members' Personal Information. Defendant knew its computer systems and technologies for
15 accepting and securing Plaintiffs' and Class Members' Personal Information had numerous
16 security vulnerabilities, but Defendant continued to collect, store, and maintain Plaintiffs' and
17 Class Members' Personal Information without fixing the vulnerabilities, even after the First
18 Data Leak.

19 188. As a result of Defendant's misconduct, Plaintiffs' and the other Class Members'
20 Personal Information was compromised – placing them at a greater risk of identity theft and
21 subjecting them to identity theft and fraud – and disclosed to unauthorized third parties without
22 their consent. Plaintiffs and the other Class Members also suffered diminution in value of their
23 Personal Information in that it became easily available to hackers on the dark web. Plaintiffs
24 and the other Class Members have also suffered consequential out-of-pocket losses for
25 procuring credit freezes or protection services, identity theft monitoring, and other expenses
26 relating to identity theft losses or protective measures.

27
28

Seventh Claim for Relief
Deceit by Concealment or Omission
(Cal. Civil Code §§ 1709, 1710)

189. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained in Paragraphs 1 through 124 as though the same were fully set forth herein.

190. Defendant's choice-of-law provision establishes that California law applies to Plaintiffs' and the other Class Members' claims.

191. As alleged above, Defendant knew that its data security measures were grossly inadequate by, at the absolute latest, March 2018. At that time, Defendant was on notice of the software glitch in Google+ that gave outside developers potential access to private Google+ User profile data – facts that Defendant should have already known given its previous exposures and security problems.

192. In response to all of these facts, Defendant chose to do nothing to protect Plaintiffs and the Class or warn them about the security problems. Instead, Defendant chose to conceal the breach in order to avoid public backlash and a Congressional inquiry. Defendant's actions thereby allowed third-party application developers to improperly collect the Personal Information of at least 53 million Google+ users

193. Defendant had an obligation to disclose to all Class Members that their Google account(s) and Personal Information were potentially compromised by the data breach.

194. Defendant made no such disclosure following the First Data Leak. Instead, Defendant willfully deceived Plaintiffs and the Class by concealing the true facts concerning its poor data security even though it was obligated to, and had a duty to, disclose those facts.

195. Had Defendant disclosed the true facts about its poor data security, Plaintiffs and the Class would have taken measures to protect themselves. Plaintiffs and the Class justifiably relied on Defendant to provide accurate and complete information about Defendant's data security, which Defendant failed to do.

1 196. Independent of any representations made by Defendant, Plaintiffs and the Class
 2 justifiably relied on Defendant to provide a service with at least minimally adequate security
 3 measures and to disclose facts undermining that reliance.

4 197. Rather than disclosing to Plaintiffs and the Class that the Google+ platform had
 5 been compromised by the breach and that Personal Information had been improperly exposed in
 6 the First Data Leak, Defendant continued with business as usual, concealing information
 7 relating to the inadequacy of its security measures from Plaintiffs and the Class.

8 198. While Defendant represented that it had fixed the vulnerability after the First
 9 Data Leak, it continued to conceal information relating to the inadequacy of its security
 10 measures, which resulted in the Second Data Leak.

11 199. These actions are “deceit” under Cal. Civil Code § 1710 in that they are the
 12 suppression of a fact, by one who is bound to disclose it, or who gives information of other facts
 13 which are likely to mislead for want of communication of that fact.

14 200. As a result of this deceit by Defendant, it is liable under Cal. Civil Code § 1709
 15 for “any damage which [Plaintiffs and the Class] thereby suffer[].”

16 201. As a result of this deceit by Defendant, the Personal Information of Plaintiffs and
 17 the Class were compromised, and their Personal Information was disclosed to third parties
 18 without their consent. Plaintiffs and the other Class Members also suffered diminution in value
 19 of their Personal Information. Plaintiffs and the Class have also suffered consequential out-of-
 20 pocket losses for procuring credit freeze or protection services, identity theft monitoring, and
 21 other expenses relating to identity theft losses or protective measures.

22 202. Defendant’s deceit, as alleged herein, is fraud under Civil Code § 3294(c)(3) in
 23 that it was a deceit or concealment of a material fact known to Defendant conducted with the
 24 intent on the part of Defendant of depriving Plaintiffs and the Class of “legal rights or otherwise
 25 causing injury.” As a result, Plaintiffs and the Class are entitled to punitive damages against
 26 Defendant under Civil Code § 3294(a).

27

28

Eighth Claim for Relief
Breach of Contract

203. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every allegation contained in Paragraphs 1 through 124 as though the same were fully set forth herein.

204. At all relevant times, Defendant and Plaintiffs mutually assented to, and therefore were bound by the version of Google’s Terms of Service and Privacy Policy (collectively, the “Contracts”) that was operative at the time each of the Plaintiffs and other Class Members joined Google+.

205. Throughout the Class Period, Defendant affirmatively stated in the Contracts that it would not disclose Google+ users' Personal Information without consent and/or notice. Defendant further represented in the Contracts that it would utilize sufficient data security protocols and mechanisms to protect Google+ users' Personal Information.

206. None of the Contracts informed and obtained Users' meaningful and lawfully obtained consent to share their content and information with third parties without their consent, or disclosed that such information would be shared if their contacts entered into an agreement which permitted third parties to collect their contacts' information.

207. Thus, per the provision above, the Contracts did not authorize Defendant to share Plaintiffs' and the other Class Members' Personal Information with third parties without their consent.

208. Plaintiffs and the other Class Members fully performed their obligations under the Contracts.

209. Defendant breached the Contracts it entered into with Plaintiffs and the other Class Members by failing to safeguard and protect their Personal Information, and improperly allowing third parties to access their Personal Information without their consent.

210. As a direct and proximate result of Google's breaches of the Contracts between Defendant and Plaintiffs and the other Class Members, Plaintiffs and the other Class Members sustained actual losses and damages, as described in detail *supra*. Plaintiffs and the other Class Members suffered injury-in-fact and lost money or property. In addition, Plaintiffs and the other

1 Class Members' Personal Information was taken and is in the hands of those who will use it for
 2 their own advantage, or is being sold for value, making it clear that the hacked information is of
 3 tangible value.

4 **Ninth Claim for Relief**

5 **Breach of Implied Covenant of Good Faith and Fair Dealing
 (In the Alternative)**

6 211. Plaintiffs hereby repeat, reallege, and incorporate by reference each and every
 7 allegation contained in Paragraphs 1 through 124 as though the same were fully set forth herein.
 8 This claim is pleaded in the alternative to the claim for breach of contract.

9 212. Defendant's choice-of-law provision establishes that California law applies to
 10 Plaintiffs' and the other Class Members' claims.

11 213. Under California law, there is in every contract or agreement an implied promise
 12 of good faith and fair dealing. Such a duty is read into contracts and functions as a supplement
 13 to the express contractual covenants, in order to prevent a transgressing party from engaging in
 14 conduct which (while not technically transgressing the express covenants) frustrates the other
 15 party's rights to the benefit of the contract. Thus, any claim on the part of Defendant that it was
 16 technically permitted to allow the collection and transmittal of Plaintiffs' and the other Class
 17 Members' Personal Information must be read in the context of, and give way to, their rights to
 18 the benefit of the contract, including the terms strictly delimiting such activity.

19 214. Defendant made specific representations to Plaintiffs and the other Class
 20 Members regarding Defendant's protection of Users' Personal Information in its Privacy Policy
 21 that was operative at the time each of the Plaintiffs and other Class Members joined Google+.

22 215. A covenant of good faith and fair dealing attaches to Defendant's Privacy Policy.

23 216. Throughout the Class Period, Defendant affirmatively stated in the Privacy
 24 Policy that it would not disclose Google+ users' Personal Information without their consent
 25 and/or notice. Defendant further represented in the Privacy Policy that it would utilize sufficient
 26 data security protocols and mechanisms to protect Google+ users' Personal Information.

217. Plaintiffs and the other Class Members fully performed their obligations under the contractual provisions in the Privacy Policy.

218. Under the terms of the Privacy Policy, Plaintiffs and the other Class Members were entitled to receive the benefits promised to them by Defendant, including that Defendant would protect their Personal Information, would not disclose their Personal Information to third parties without their consent, and would keep their Personal Information secure.

219. Defendant was uniquely able to control the rights of its Users, including Plaintiffs and the other Class Members, concerning their privacy, ownership, and control of its content and information, and whether that content and information would be provided to third parties without their consent.

220. Defendant surreptitiously took measures to frustrate and undercut Plaintiffs' and the other Class Members' contractual rights concerning their privacy, ownership, and control over their Personal Information, and whether their content and information would be provided to third parties without their consent. By doing so, Defendant deprived Plaintiffs and the other Class Members of the benefits under their contracts with Defendant, including the Privacy Policy.

221. As a direct and proximate result of Defendant's breaches of its duty of good faith and fair dealing, Plaintiffs and the other Class Members sustained actual losses and damages, as described in detail *supra*. Plaintiffs and the other Class Members suffered injury-in-fact and lost money or property. In addition, their Personal Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class Members, respectfully request that this Court enter an Order:

a. Certifying the Class, appointing Plaintiffs as Class Representatives, and appointing the law firms of Franklin D. Azar & Associates and Morgan & Morgan Complex Litigation Group as Class Counsel;

- 1 b. Finding that Defendant's conduct was negligent, deceptive, unfair, and unlawful
2 as alleged herein;
- 3 c. Enjoining Defendant from engaging in further negligent, deceptive, unfair, and
4 unlawful business practices as alleged herein;
- 5 d. Awarding Plaintiffs and the other Class Members actual, compensatory, nominal,
6 and consequential damages;
- 7 e. Awarding Plaintiffs and the other Class Members statutory damages and
8 penalties, as allowed by law;
- 9 f. Awarding Plaintiffs and the other Class Members restitution and disgorgement;
- 10 g. Requiring Defendant to provide appropriate credit monitoring services to
11 Plaintiffs and the other Class Members;
- 12 h. Awarding Plaintiffs and the other Class Members punitive damages;
- 13 i. Awarding Plaintiffs and the other Class Members pre-judgment and post-
14 judgment interest;
- 15 j. Awarding Plaintiffs and the other Class Members reasonable attorneys' fees
16 costs and expenses, and;
- 17 k. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

19 Plaintiffs demand a trial by jury of all claims in this Amended Consolidated Class
20 Action Complaint so triable.

1
2 Dated: March 1, 2019
3
4
5
6
7

/s/ John A. Yanchunis

John A. Yanchunis (*pro hac vice*)

Jonathan B. Cohen (*pro hac vice*)

Ryan J. McGee (*pro hac vice*)

Morgan & Morgan

Complex Litigation Group

Clayeo C. Arnold (65070)

Clayeo C. Arnold, P.C.

Counsel for Plaintiffs Matic and Harris

Ivy T. Ngo (249860)

Franklin D. Azar & Associates, P.C.

Counsel for Plaintiffs Olson and Pinkowski

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28